UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/673,698	09/29/2003	Tong-Ming Lee	15436.187	4165

22913 7590 04/06/2007

WORKMAN NYDEGGER
(F/K/A WORKMAN NYDEGGER & SEELEY)
60 EAST SOUTH TEMPLE
1000 EAGLE GATE TOWER
SALT LAKE CITY, UT 84111

EXAMINER	
PICH, PONNOREAY	
ART UNIT	**PAPER NUMBER**
2135	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/673,698	LEE ET AL.	
	Examiner	Art Unit	
	Ponnoreay Pich	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 August 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *8/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-30 have been examined and are pending.

Information Disclosure Statement

The IDS submitted on 8/23/2004 has been considered.

Claim Objections

Claims 1-4, 8, 9, 12, 14, and 20-23 are objected to because of the following informalities:

1. Claim 1 recites "said analyzer" in the last line which should be "said at least one network analyzer" so as to be consistent with what was earlier recited. Claim 14 contains a similar informality.
2. Claim 1 recites "said keyset profile" in line 8, which should be "said single keyset profile". Claims 14 and 20-22 contain a similar informality.
3. Claims 2, 3, 4, 8, and 12 recite "said profile" which should instead be "said single keyset profile" so as to be consistent with what is recited in claim 1.
4. "providing" in line 9 of claim 23 appears to be a typo. The examiner assumes it should be deleted.
5. Claim 9 is improperly dependent on itself. It is assumed that claim 9 should depend on claim 8.
6. As per claim 21, the examiner believes "downloads" should be recited instead of "uploads".
7. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-13 and 23-30 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

1. "said profile containing said keyset to each of said plurality of access points" recited in the last 2 lines of claim 2 is indefinite. It appears applicant may have misworded the limitation.
2. "said keysets" recited in claim 1 lacks antecedent basis. Subsequent recitation of "said keysets" in claims dependent on claim 1 also lack antecedent basis, i.e. see claims 4-7.
3. Claim 10 recites "said computer" which lacks antecedent basis.
4. "said keyset" in lines 8-9 of claim 23 lacks antecedent basis.
5. Claim 25 recites "said encrypted data". It is unclear to which encrypted data is being referred, i.e. the ones recited in claim 23 or the ones recited in claim 25.
6. Any claims not specifically addressed are rejected by virtue of dependency. Applicant is respectfully advised to check for any other informalities or indefinite limitations that the examiner may have inadvertently missed.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-2, 14, 16, and 20-21 are rejected under 35 U.S.C. 102(b) as being anticipated by Balogh US 2001/0024953).

Claim 1:

Balogh discloses a computer network system having wireless components providing encrypted data transmission and receipt and comprising at least two wireless access points (Fig 1), said network having a different encryption keyset for each of said at least two access points (Fig 2 and paragraphs 24, 27, and 43). Paragraph 24 discusses how each information sets can be called profiles. Figure 2 and paragraph 27 show how each information set/profile has WEP keys associated with them. Paragraph 43 discusses how a second access point may use a different information set/profile than a first access point.

Balogh discloses at least one network analyzer (Fig 1, MS) connected to said network by a wireless network card (Fig 1 and paragraph 18), said network analyzer being adapted to decrypt data captured from said at least one of said at least two access points by said wireless network card (Fig 3 and paragraphs 27 and 35) wherein each of said keysets is grouped into a single keyset profile (Fig 2), said single keyset profile being used to decrypt all of said captured data without having to enter a key or keyset information into said at least one network analyzer (paragraph 29).

Note that paragraph 35 discusses that what is shown in Figure 3 is the mobile station communicating on the network of Figure 1 in infrastructure mode, which means the mobile station connects to the network via access points. Further, because WEP encryption is enabled on the network, communication between the access points and mobile station are encrypted, which implies decryption of the communication packets once the mobile station receives the packets from the access points.

Claim 2:

Balogh further discloses a plurality of access points (Fig 1, AP1-4), each access point having a keyset that encrypts data to and from at least one user and said access point (paragraphs 27 and 35), said single keyset profile containing said keyset to each of said plurality of access points (Fig 2 and paragraphs 33-34).

With a wireless network operation in infrastructure mode that uses encryption, both the mobile station and the access points each contain the keys/keysets needed to encrypt and decrypt packets sent between each other.

Claim 14:

Balogh discloses:

1. At least one wireless card adapted to communicate with the at least two wireless access points and capture data from the at least two wireless access points (Fig 1, MT and paragraph 18).
2. A single keyset profile having a plurality of encryption keysets (Fig 2 and paragraph 24).

The rest of what is recited in claim 14 which details how the keyset and keyset profiles are used are not given patentable weight. As per MPEP 2114-2115, the patentability of an apparatus depends on its structure and not how it is used or any materials intended to be used with the apparatus. The limitations dealing with how the keyset and keyset profile are being used do not further define the structure of the claimed network analyzer.

Claim 16:

Balogh further discloses wherein each encryption keyset comprises at least two keys (Fig 2). Note the information set/profile shown in Figure 2 refers to keys.

Claim 20:

Balogh further discloses wherein said single keyset profile is stored on a computer accessible through said network (paragraph 29).

Claim 21:

Balogh further discloses wherein said network analyzer downloads said single keyset profile from said computer (paragraph 29).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

> invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 3, 17, and 23-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Balogh US 2001/0024953).

Claim 3:

Balogh does not explicitly disclose in his invention wherein each access point utilizes a unique keyset, and wherein each single keyset profile contains each unique key set. However, Balogh discloses it was well known in the art to use different keys for different network (paragraph 3). Balogh discloses the network of Figure 1 being comprised of separate subnetworks (paragraphs 27 and 43).

At the time applicant's invention was made, it would have been obvious to modify Balogh's invention according to the limitations recited in claim 3 such that each access point utilizes a unique keyset, and wherein each single keyset profile contains each unique key set in light of what Balogh teaches as being well known in the art. One skilled would have been motivated to do so because different keys are typically utilized in different networks (paragraph 3) and it would be more secure if each network used different keys.

Claim 17:

Balogh does not explicitly disclose in his invention wherein each key is unique. However, Balogh discloses it was well known in the art to use different keys for different network (paragraph 3). Balogh discloses the network of Figure 1 being comprised of separate subnetworks (paragraphs 27 and 43).

At the time applicant's invention was made, it would have been obvious to one skilled in the art to modify Balogh's invention such that each key is unique. One skilled would have been motivated to do so because different keys are typically utilized in different networks (paragraph 3) and it would be more secure if each network used different keys.

Claim 23:

Balogh discloses:

1. A step for establishing a keyset profile accessible by said analyzer module, said keyset having all keysets having all keysets being used by any of said at least two access points (paragraphs 24, 27, and 31).
2. A step for receiving data from at least one of said at least two access points (paragraph 51).

Balogh does not explicitly disclose the received data is encrypted and does not explicitly disclose a step for decrypting said received data by using said keyset profile, wherein said data is decrypted without manually entering keys or keystep information. However, WEP is utilized by Balogh's invention (paragraphs 22 and 27). This means that data sent between the mobile station and access point are encrypted and are decrypted once they reach their destination using the keyset profile. The multiple profiles are chosen automatically, thus data are decrypted without manually entering keys or keystep information (paragraph 33).

At the time applicant's invention was made, it would have been obvious to modify Balogh's invention as recited in claim 23. One skilled would have been motivated to do so because use of WEP means that data are sent in encrypted format and decrypted once it reaches its destination.

Claim 24:

Balogh does not explicitly disclose storing said decrypted data. However, official notice is taken that storing decrypted data was well known in the art at the time applicant's invention was made. It would have been obvious to modify Balogh's invention to store decrypted data. One skilled would have been motivated to store decrypted data so as to be able to use the data later without having to redownload.

Claim 25:

Balogh does not explicitly disclose a step for analyzing said decrypted data to identify any encrypted data. However, official notice is taken that data being encrypted multiple times (i.e. 3DES), thus requiring multiple levels of decryption, were well known in the art at the time applicant's invention was made. It would have been obvious to further modify Balogh's invention to include a step for analyzing said decrypted data to identify any encrypted data. One skilled would have been motivated to do so as it would allow one to identify any decryption error as well as identify data that requires further decryption.

Claim 26:

As per claim 26, official notice was taken in claim 25 that multiple levels of encryption was well known in the art, i.e. 3DES. As such, it would have been obvious to

also modify Balogh's invention to include a step for decrypting said encrypted data using a second keyset associated with said keyset profile. One skilled would have been motivated to do so because it would allow proper decryption of any packets that were encrypted multiple times or had errors during decryption and still requires decryption.

Claim 27:

Balogh further discloses a step for selecting said keyset profile for said at least two wireless access points (paragraph 33).

Claim 28:

Balogh further discloses a step for accessing said keyset profile at a location of said computer network remote from said analyzer module (paragraph 29).

Claim 29:

As per claim 29, Balogh does not explicitly disclose a step for decrypting said keyset profile and storing a decrypted version of said keyset profile local to said analyzer module. However, official notice is taken that decrypting data and storing a local version in decrypted form was well known in the art at the time applicant's invention was made. It would have been obvious to one skilled in the art to modify Balogh's invention according to the limitations recited in claim 29. One skilled would have been motivated to do so because the analyzer module needs a decrypted version of the keyset to enable proper communication between it and an access point.

Claims 4-13, 15, 18-19, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Balogh US 2001/0024953) in view of Whelan et al (US 2003/0219129).

Claim 4:

Balogh does not explicitly disclose wherein said keyset for each access point utilizes at least two keys, and wherein said single keyset profile contains each of said keyset. However, Whelan discloses the limitation (Fig 2, items 22).

At the time applicant's invention was made, it would have been obvious to one skilled in the art to modify Balogh's invention according to the limitations recited in claim 4 by incorporating Whelan's teachings. One skilled would have been motivated to do so because it would increase the security of the Balogh's wireless network because Whelan's teachings would make it impractical for a hacker to gather sufficient information to using any one key to decrypt the key (Whelan: paragraph 16).

Claim 5:

Balogh does not explicitly disclose wherein each of said keysets is unique. However, Balogh discloses it was well known in the art to use different keys for different network (paragraph 3). Balogh discloses the network of Figure 1 being comprised of separate subnetworks (paragraphs 27 and 43).

At the time applicant's invention was made, it would have been obvious to one skilled in the art to modify Balogh's invention such that each of said keysets is unique. One skilled would have been motivated to do so because it is typical practice in the art for each network to have a unique keyset. This makes each network more secure.

Claim 6:

As per claim 6, Whelan further discloses wherein each of said keysets uses at least 64 bit encryption (paragraph 131)

Claim 7:

As per claim 7, Whelan further discloses wherein each of said keysets uses at least 128 bit encryption (paragraph 131).

Claim 8:

Balogh further discloses wherein said single keyset profile is a file and said file is stored internally in said network analyzer (paragraphs 24 and 29). Whelan also discloses the limitation Fig 1, item 28 and paragraph 55).

Claim 9:

Balogh does not explicitly disclose wherein said file is stored in an encrypted form on said network analyzer. However, Whelan discloses storing the file containing said list of keys in encrypted form (paragraph 120). At the time applicant's invention was made, it would have been obvious to one skilled in the art to further modify Balogh's invention such that the file is stored in an encrypted form on said network analyzer. One skilled would have been motivated to do so because encrypting the file increases security for the network.

Claim 10:

As per claim 10, Whelan further discloses wherein said profile is a file and said file is stored on said computer (paragraph 120).

Claim 11:

As per claim 11, Whelan further discloses wherein said file is stored in an encrypted form on said computer (paragraph 120).

Claim 12:

Balogh further discloses wherein said profile is a file and said file is stored on said network (paragraph 29).

Claim 13:

As per claim 13, Whelan further discloses wherein said file is stored in an encrypted form on said network (paragraph 120).

Claim 15:

Balogh does not explicitly disclose wherein each encryption keyset of said plurality of encryption keysets is a unique keyset. However, Whelan discloses updating and replacing keysets (paragraph 145). In light of this teaching, it would have been obvious to one skilled in the art to modify Balogh's invention such that each encryption keyset of said plurality of encryption keysets is a unique keyset. One skilled would have been motivated to do so because frequently rotating keysets with newer keysets periodically makes it impractical for a hacker to gain sufficient network traffic using any one key to decrypt the key (Whelan: paragraph 16).

Claim 18:

Balogh does not explicitly disclose wherein each of said plurality of keysets uses at least 64 bit encryption. However, Whelan discloses keys being at least 64 bit (paragraph 131). At the time applicant's invention was made, it would have been obvious to one skilled in the art to modify Balogh's invention such that each of said

plurality of keysets uses at least 64 bit encryption. One skilled would have been motivated to do so because larger key sizes allows for stronger encryption.

Claim 19:

Balogh does not explicitly disclose wherein each of said plurality of keysets uses at least 128 bit encryption. However, Whelan discloses keys being at least 128 bit (paragraph 131). At the time applicant's invention was made, it would have been obvious to one skilled in the art to modify Balogh's invention such that each of said plurality of keysets uses at least 128 bit encryption. One skilled would have been motivated to do so because larger key sizes allows for stronger encryption.

Claim 22:

Balogh does not explicitly disclose wherein said single keyset profile is stored in an encrypted form on said computer. However, Whelan discloses storing keyset profiles in encrypted form on a network computer (paragraph 120).

At the time applicant's invention was made, it would have been obvious to one skilled in the art to modify Balogh's invention according to the limitations recited in claim 22. One skilled would have been motivated to do so because storing keys in encrypted form would make Balogh's network more secure.

Claim 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over Balogh US 2001/0024953) in view of Cafarelli et al (US 6,697,337).

Claim 30:

As per claim 30, Balogh does not explicitly disclose a step for displaying said decrypted data through at least one user interface. However, Cafarelli discloses the limitation (col 7, lines 41-52 and col 12, lines 19-56). At the time applicant's invention was made, it would have been obvious to one skilled in the art to modify Balogh's invention according to the limitations recited in claim 30. One skilled would have been motivated to display decrypted data through at least one user interface because it would allow a user to troubleshoot various problem with the wireless network and improve the network (col 12, lines 56-62).

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claim 14 is provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 1 of copending Application No. 10/713,219. The main differences between the two claims is that claim 1 of the '219 application additionally recites that the wireless card receives encrypted data on one or more channel and that the single keyset profile is stored in a data store. However, since the keyset profile recite in claim 14 of the current application is used to decrypt encrypted data received from different access points, it is obvious that the data received by the at least one wireless card of the current application is also encrypted and the keyset profile of the current application must be stored in a data store of the network analyzer since keyset profile is a component of the network analyzer.

Claims 23, 25, 28, and 30 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 15, 17, 22, and 24 respectively of copending Application No. 10/713,219. The main difference is that in independent claim 15 of the '219 application, encrypted data is saved to a data store in the second step. However, saving encrypted data to a data store was well known in the art and it would have been obvious to modify the claims of the current application such that encrypted data are saved to a data store. One skilled would have been motivated to do so because it would allow buffered processing of received data.

This is a provisional obviousness-type double patenting rejection.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Thurs.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Ponnoreay Pich
Examiner
Art Unit 2135

HOSUK SONG
PRIMARY EXAMINER

PP